BY ORDER OF THE COMMANDER
AIR RESERVE PERSONNEL CENTER

AIR FORCE INSTRUCTION 33-115, VOLUME 2

ARPC
Supplement 1

14 OCTOBER 2004

Communications and Information

LICENSING NETWORK USERS AND CERTIFYING NETWORK PROFESSIONALS

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at: **http://www.e-publishing.af.mil.**

OPR: HQ ARPC/SCON (Ms Marion Seamster)

Certified by: HQ ARPC/SC
(Mr. Stephen J. Hannan)
Pages: 2
Distribution: F

This supplement implements and extends the guidance of AFI 33-115, Volume 2, 14 April 2004. The AFI is published word-for-word without editorial review. Air Reserve Personnel Center (ARPC) supplementary material is indicated by "(ARPC)" in boldface type. This supplement describes ARPC procedures to be used in conjunction with the basic instruction. Upon receipt of this integrated supplement discard the Air Force basic.

5.6.1. Procedural Requirements: In the event that an ARPC network user (identified by their user-ID) is suspected of abusing network resources, the ARPC Information Assurance Manager will validate the user-ID and provide support documentation. Once it has been determined that the individual undeniably violated the ARPC System Security Policy, that individual's access to the ARPC network will be suspended.

5.6.1.3. (Added) In order for the offender to regain access to the ARPC network:

5.6.1.3.1. (Added) **First Offense** : Offender must re-accomplish Information Awareness training plus submit a letter/e-mail from the offender's supervisor to the Designated Approval Authority (DAA) outlining actions taken to prevent a reoccurrence of the network violation.

5.6.1.3.2. (Added) **Second Offense** : Offender must re-accomplish Information Awareness training plus submit a letter/e-mail from the offender's Director to the DAA outlining actions taken to prevent a reoccurrence of the network violation.

5.6.1.3.3. (Added) **Third Offense** : The DAA will consult with the ARPC commander to determine if network access will be permanently revoked.

5.6.3. (Added) The Chief, Network Control Center, is authorized to suspend network privileges and/or delete accounts as required to protect the performance and integrity of the ARPC network. All offenders will be required to re-accomplish the mandatory annual Information Assurance training before access to the network is restored. Additionally, any violation may subject the military member to punishment under

Articles 90, 91, 92, 133, and 134 of the Uniform Code of Military Justice. Violations by civilian employees may result in administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws.

5.8. (Added) All government communication systems and equipment (including Government owned telephones, facsimile machines, e-mail, internet systems, and commercial systems when used is paid for by the Federal Government) shall be for official use and authorized purposes only, as stated in AFI 33-119, *Electronic Mail (E-mail) Management and Use*, and AFI 33-115 Volume 2. The following list contains examples of prohibited e-mail and internet actions. These actions are prohibited because they increase vulnerabilities or limit network capability provided to the war fighter. Abuse of network resources is categorized as intentional or unintentional (person did not understand the consequences of their actions). ***NOTE***: This list is not all inclusive of unapproved actions nor is it prioritized.

5.8.1. (Added) Forwarding unofficial e-mails to "ALL" groups. This action usually results in a denial of service and limits the capability of personnel to accomplish the mission.

5.8.2. (Added) Accessing, storing, processing, displaying, distributing, transmitting, or viewing inappropriate material such as pornography, racist material, material promoting hate crimes, or material which may have adverse effects on good order and discipline.

5.8.3. (Added) Visiting, participating in, or downloading files from gaming, chat, or hacker sites.

5.8.4. (Added) Obtaining, installing, copying, pasting, transferring or using software or other materials obtained in violation of the appropriate vender's patent, copyright, trade secret, license agreement, or software obtained through other than official means i.e., software from home.

5.8.5. (Added) Data streaming applications (e.g., RealPlayer, Yahoo, MSN, CNN, or ESPN audio/video, PointCast, etc.) will be used only for authorized official business.

5.8.6. (Added) Attempting to circumvent or defeat security or auditing systems without prior authorization or permission.

5.8.7. (Added) Downloading or installing on your government computer freeware, shareware, peer-to-peer, or beta software programs to include programs such as Kazaa, Bearwear, Imesh, Metafiles, screensavers, JPEGs/MPEGs, and games of any kind.

JAMES L. PLAYFORD, Colonel, USAF
Commander